



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/603,209	06/25/2003	Ulrich Emmerling	071308.0443	2679

31625 7590 06/29/2007
BAKER BOTTS L.L.P.
PATENT DEPARTMENT
98 SAN JACINTO BLVD., SUITE 1500
AUSTIN, TX 78701-4039

EXAMINER

DWIVEDI, MAHESH H

ART UNIT	PAPER NUMBER
----------	--------------

2168

MAIL DATE	DELIVERY MODE
-----------	---------------

06/29/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

MAILED

JUN 29 2007

Technology Center 2100

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 10/603,209

Filing Date: June 25, 2003

Appellant(s): EMMERLING ET AL.

Andreas Grubert

For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 02/20/2007 appealing from the Office action mailed 08/28/2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

4,509,093	Stellberger	04/02/1985
6,381,699	Kocher et al.	04/30/2002

(9) Grounds of Rejection

Art Unit: 2168

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-2, and 11 are rejected under 35 U.S.C. 102(b) as being anticipated by **Stellberger** ("Stellberger" (U.S. Patent 4,509,093)).

Regarding claim 1, **Stellberger** teaches a method comprising:

a) transmitting an item of information unidirectionally between the first object and the at least one further object (Column 6, lines 60-67-Column 7, lines 1-8);

b) calculating a computation result in the relevant receiving object from parts of the transmitted information (Column 7, lines 9-23);

c) comparing the calculated computation result with a computation result transferred with the information in the relevant receiving object, (Column 4, lines 22-27, Column 9, lines 32-36); and

d) authenticating the first object to the at least one further object only if there is a match between the calculated computation result and transferred computation result, and declaring the computation result as invalid for further transmissions (Column 5, lines 29-31, Column 8, lines 4-12).

The examiner notes that **Stellberger** teaches that the comparison phase can be performed on either the key or the lock. The examiner further notes that "The comparison phase between the output signals produced in each working cycle is preferable made alternately in the key part and then in the lock part" (Column 4, lines 22-27) is analogous to "**comparing the calculated computation result with a computation result transferred with the information in the relevant receiving object**". The examiner further notes that it is common knowledge that "random-access memory" (Column 5, lines 29-30) is refreshed after each cycle of inputting data. The

Art Unit: 2168

examiner further notes that refreshing the data is analogous to declaring the data as “invalid”.

Regarding claim 2, **Stellberger** further teaches a method comprising:

- A) wherein the first object comprises a vehicle and the least further object comprises a key; and (Column 5, lines 58-61).
- B) wherein the information is transmitted from the vehicle and received by the key (Column 5, lines 58-61).

Regarding claim 11, **Stellberger** teaches a method comprising:

- a) transmitting an item of information unidirectionally between the vehicle and the key (Column 6, lines 60-67-Column 7, lines 1-8);
- b) calculating a computation result in the key from parts of the transmitted information (Column 7, lines 9-23);
- c) comparing the calculated computation result with a computation result transferred with the information, wherein the comparing is in the key (Column 4, lines 22-27, Column 9, lines 32-36); and
- d) authenticating the vehicle if there is a match between the calculated computation result and the transferred computation result, and declaring the computation result as invalid for further transmissions (Column 5, lines 29-31, Column 8, lines 4-12).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of

Art Unit: 2168

the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

4. Claims 3-10, and 12-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Stellberger** (U.S. Patent 4,509,093) and in view of **Kocher et al.** (U.S. Patent 6,381,699).

5. Regarding claim 3, **Stellberger** teaches a method comprising:

A) a random number (Column 5, lines 29-31)

Stellberger, however, does not teach:

B) an incremental or decrementable item of data, wherein the incremental or decremental item of data is stored in the at least one further object if the calculated computation result matches the transferred computation result; and

C) wherein after each transmission of the information, regardless of a successful receipt, the item of data is incremented or decremented before new information is transmitted (Kocher, Column 9, lines 23-45).

Kocher, however, teaches “an incremental or decrementable item of data, wherein the incremental or decremental item of data is stored in the at least one further object if the calculated computation result matches the transferred computation result” as “sends other needed information (such as data or t) to the verifier” (Column 9, lines 23-45), and “wherein after each transmission of the information, regardless of a successful receipt, the item of data is incremented or decremented before new information is transmitted” as “if t matches, the verifier increments t” (Column 9, lines 23-45).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Kocher's** would have allowed **Stellberger's** provide a system of security that remains

secure even if attackers gather some information about the system, as noted by **Kocher** (Column 2, lines 40-44).

Regarding claim 4, **Stellberger** teaches a method comprising:

A) a random number (Column 5, lines 29-31)

Stellberger, however, does not teach:

B) an incremental or decrementable item of data, wherein the incremental or decremental item of data is stored in the key if the calculated computation result matches the transferred computation result; and

C) wherein after each transmission of the information, regardless of a successful receipt, the item of data is incremented or decremented before new information is transmitted (Kocher, Column 9, lines 23-45).

Kocher, however, teaches “an incremental or decrementable item of data, wherein the incremental or decremental item of data is stored in the key if the calculated computation result matches the transferred computation result” as “sends other needed information (such as data or t) to the verifier” (Column 9, lines 23-45), and “wherein after each transmission of the information, regardless of a successful receipt, the item of data is incremented or decremented before new information is transmitted” as “if t matches, the verifier increments t” (Column 9, lines 23-45).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Kocher's** would have allowed **Stellberger's** provide a system of security that remains secure even if attackers gather some information about the system, as noted by **Kocher** (Column 2, lines 40-44).

Regarding claims 5-6, and 13, **Stellberger** does not explicitly teach a method comprising:

A) wherein a counter state or item of time data is transferred as the item of data that can be incremented.

Kocher, however, teaches “**a counter state or item of time data is transferred as the item of data that can be incremented**” as “counter t” (Column 9, line 24).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Kocher's** would have allowed **Stellberger's** provide a system of security that remains secure even if attackers gather some information about the system, as noted by **Kocher** (Column 2, lines 40-44).

Regarding claims 7 and 14, **Stellberger** does not explicitly teach a method comprising:

A) wherein the result is only calculated when the transferred item of data is greater than the stored item of data.

Kocher, however, teaches “**wherein the result is only calculated when the transferred item of data is greater than the stored item of data**” as “if the received value of t is larger than the internal value but the difference is not unreasonably large, it may be appropriate to accept the signature” (Column 9, lines 38-45).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Kocher's** would have allowed **Stellberger's** provide a system of security that remains secure even if attackers gather some information about the system, as noted by **Kocher** (Column 2, lines 40-44).

Regarding claims 8-9, and 15-16, **Stellberger** does not explicitly teach a method comprising:

A) wherein when the transferred result and the calculated result match, the incrementable item of data is increased so that the transferred result becomes invalid (Column 9, lines 23-45).

Kocher, however, teaches “**wherein when the transferred result and the calculated result match, the incrementable item of data is increased so that the transferred result becomes invalid**” as “if t matches” (Column 9, lines 38-45).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Kocher's** would have allowed **Stellberger's** provide a system of security that remains secure even if attackers gather some information about the system, as noted by **Kocher** (Column 2, lines 40-44).

Regarding claims 10 and 17, **Stellberger** does not explicitly teach a method comprising:

A) wherein the result is computed in at least one further object using a cryptological computation algorithm known there and a code word (Column 9, lines 8-22).

Kocher, however, teaches "a code word" as "symmetrically signed-code" (Column 9, line 10), and "wherein the result is computed in at least one further object using a cryptological computation algorithm known there" as "a hash or Mac of the data is typically computed using a secret key" (Column 9, lines 11-22).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Kocher's** would have allowed **Stellberger's** provide a system of security that remains secure even if attackers gather some information about the system, as noted by **Kocher** (Column 2, lines 40-44).

Regarding claim 12, **Stellberger** teaches a method comprising:

A) a random number (Column 5, lines 29-31)

B) key (Column 5, lines 58-61)

Stellberger, however, does not teach:

B) an incremental or decrementable item of data, wherein the incremental or decremental item of data is stored in the key if the calculated computation result matches the transferred computation result; and

C) wherein after each transmission of the information, regardless of a successful receipt, the item of data is incremented or decremented before new information is transmitted.

Kocher, however, teaches “an incremental or decrementable item of data which is stored in the key if it matches the computation result, is transferred” as “sends other needed information (such as data or t) to the verifier” (Column 9, lines 23-45), and “wherein after each transmission of the information, regardless of a successful receipt, the item of data is incremented or decremented before new information is transmitted” as “if t matches, the verifier increments t” (Column 9, lines 23-45).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Kocher's** would have allowed **Stellberger's** provide a system of security that remains secure even if attackers gather some information about the system, as noted by **Kocher** (Column 2, lines 40-44).

(10) Response to Argument

A. Claims 1-2, and 11 are rejected under 35 U.S.C. 102(b) as being anticipated by Stellberger (U.S. Patent 4,509,093)

1. Independent Claims 1 and 11

Arguments (1): Regarding Independent Claims 1 & 11, Appellant argues that the “The Examiner finally rejected independent claims 1 and 11 under 35 USC 102 (a) as being anticipated by Stellberger.

However, the examiner wishes to state that the 102 rejection was made as a 102 (b) rejection, and that the indication of 102 (e) in the previous office actions was a typographical error. Moreover, the examiner further wishes to state that the statutory paragraph preceding the preamble is that of a 102 (b) rejection.

Arguments (2): Regarding Independent Claims 1 & 11, Appellant argues that “Stellberger generally discloses two different methods of authentication. The first method is represented in Fig. 2 of Stellberger and the second method in Fig. 3 of Stellberger. These methods are each distinct in their functionality and, thus, the respective steps of these method cannot simply be mixed or interchanged without comprising the functionality of the methods”.

However, the examiner wishes to recite from the MPEP: "In other words, for anticipation under 35 U.S.C. 102, the reference must teach every aspect of the claimed invention either explicitly or impliedly" (Section 706.02 [R-3] Section IV).

The examiner further wishes to state that since each and every limitation is broadly taught within the four corners of the Stellberger reference, then as a result, broadly anticipates the independent claims.

The examiner further wishes to point to Column 12 of Stellberger, which states "It will be understood that each of the elements described above, or **two or more together**, may also find useful applications in other types of constructions" (Column 12, lines 32-35). The examiner further wishes to state that as a result, Stellberger clearly teaches that flowcharts I and II may be interchanged.

Arguments (3): Regarding Independent Claims 1 & 11, Appellant argues that "In the rejection, the Examiner impermissibly identifies different steps of the two Stellberger methods and mixes these steps to create a new method which is not disclosed or suggested in Stellberger. For example, citations I, II, and V relate to the first method shown in Fig. 2. However, citation II and IV clearly refer to the second method as shown in Fig. 3. The examiner impermissibly randomly singles out a step of the second method and tries to combine it with the first method. However, such an analysis/conclusion is neither supported by 35 USC §102 or § 103. As discussed above, first and second method perform different steps that cannot be interchanged".

However, the examiner wishes to recite from the MPEP: "In other words, for anticipation under 35 U.S.C. 102, the reference must teach every aspect of the claimed invention either explicitly or impliedly" (Section 706.02 [R-3] Section IV).

The examiner further wishes to state that since each and every limitation is broadly taught within the four corners of the Stellberger reference, then as a result, broadly anticipates the independent claims.

The examiner further wishes to point to Column 12 of Stellberger, which states "It will be understood that each of the elements described above, or **two or more together**, may also find useful applications in other types of constructions" (Column 12,

lines 32-35). The examiner further wishes to state that as a result, Stellberger clearly teaches that flowcharts I and II may be interchanged.

Arguments (4): Regarding Independent Claims 1 & 11, Appellant argues that "if according to Stellberger's first method shown in Fig. 2, step D is regarded as step a) of Claim 1 and 11, then lock unit 20 represents the first object and key unit 10 represents the at least one further object. However, the comparison which is performed in step K of Stellberger is also performed in the lock unit 20. Thus, Stellberger's first method cannot anticipate Claims 1 and 11".

However, the examiner wishes to state that the comparison limitation was cited in Stellberger as "The comparison phase between the output signals produced in each working cycle is preferably made alternately in the key part and then in the lock part" (Column 4, lines 24-27). The examiner further wishes to state that since the comparison phase is performed in the key part of Stellberger (i.e. the at least further object), then as a result, Stellberger broadly teaches "comparing the calculated computation result with a computation result transferred with the information in the relevant receiving object". Moreover, since the comparison phase is first made in the key part (see "is preferable made in the key part and then in the lock part").

Arguments (5): Regarding Independent Claims 1 & 11, Appellant argues that "Stellberger teaches to perform another separate transmission step J1 to transfer the comparison result Y-1 from the lock unit 20 to key unit 10...the method of Stellberger needs to perform a bidirectional transfer in step Dn in which information is transferred from key unit 10 to lock unit 20 and vice versa. Thus, the second method does neither disclose step a) nor step c) of independent claims 1 and 11".

However, the examiner wishes to state that the comparison limitation was cited in Stellberger as "The comparison phase between the output signals produced in each working cycle is preferably made alternately in the key part and then in the lock part" (Column 4, lines 24-27). The examiner further wishes to state that since the comparison phase is performed in the key part of Stellberger (i.e. the at least further object), then as a result, Stellberger broadly teaches "comparing the calculated computation result with a computation result transferred with the information in the

Art Unit: 2168

relevant receiving object". Moreover, since the comparison phase is first made in the key part (see "is preferable made in the key part and then in the lock part").

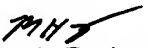
In addition, the examiner further wishes to state that independent claims 1 and 11 merely recite the limitation "comparing the calculated computation result with a computation result transferred with the information in the relevant receiving object". Since the comparison phase is first performed in the key part, then as a result, Stellberger's method broadly teaches the aforementioned limitation because a comparison is made in the relevant receiving object (i.e. the key).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,


Mahesh Dwivedi
Patent Examiner
AU 2168

Tim Vo
Supervisory Patent Examiner
AU 2168


Pierre Vital
Supervisory Patent Examiner
AU 2169


TIM VO
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100